UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,805	07/08/2005	Laurent Faillenot	GRYN 224-US	8153

24972 7590 04/04/2008
FULBRIGHT & JAWORSKI, LLP
666 FIFTH AVE
NEW YORK, NY 10103-3198

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
04/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/541,805	FAILLENOT ET AL.	
	Examiner	Art Unit	
	Christian LaForgia	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *47-92* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *47-61,63-84 and 86-92* is/are rejected.

7)☒ Claim(s) *62 and 85* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 July 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/8/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-46 have been cancelled as per Applicant's preliminary amendment.

2. Claims 47-92 have been presented for examination.

Priority

3. Acknowledgment is made of applicant's claim for foreign priority.

Information Disclosure Statement

4. The information disclosure statement filed 08 July 2005 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 47-55, 60, 61, 63-78, 83, 84, and 86-92 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 7,143,439 B2 to Cooper et al., hereinafter Cooper.

7. As per claims 47 and 70, Cooper teaches a method and system for analyzing or selectively modifying or filtering data packets passing through a device placed on an edge in a computer network (column 6, lines 58-61, i.e. a perimeter element allows access to and from

communities of hosts outside a policy domain), said device comprising a processor that runs a compiler (Figure 1A [blocks 150, 151]) and a piece of software in accordance with a security policy (Figure 1A [block 105]), said software being designed to filter said data packets, thereby authorizing or not authorizing their passage in accordance with said security policy (column 4, lines 15-23, i.e. monitoring and auditing a network's activity in additional to traditional access/denial authorization decisions), the method comprising the steps of:

defining said security policy by portable agents written in a computer language that is independent of the language of said processor and for analyzing, selectively modifying or selectively filtering said data packets (Figure 1 [block 110], column 4, lines 24-44, column 8, lines 40-58, column 14, line 25 to column 15, line 4, column 41, lines 53-57, column 43, lines 27-45);

automatically calling said compiler by said software in order to perform a compilation for translating said portable agents into executable agents written in the language of said processor (Figure 1A [blocks 106, 150], column 9, lines 51-64, column 17, lines 28-35);

running said software in order to filter said data packets passing through said device, thereby authorizing or not authorizing their passage in accordance with said security policy (Figure 1A [blocks 106, 127], column 4, lines 15-23, column 8, line 60 to column 9, line 47, column 15, lines 7-47, i.e. monitoring and auditing a network's activity in additional to traditional access/denial authorization decisions); and performing at least one of the following steps:

analyzing said data packets authorized by said software to pass through said device, by executing said executable agents by said processor (column 39, lines 61-64, column 40, lines 26-29, i.e. monitoring network traffic, analyzing full packets);

selectively modifying said data packets authorized by said software to pass through said device, by executing said executable agents by said processor (column 9, lines 16-30, column 40, lines 29-31, i.e. removing sensitive data such as passwords); or

selectively filtering said data packets authorized by said software to pass through said device, by executing said executable agents by said processor (column 4, lines 15-23, i.e. monitoring and auditing a network's activity in additional to traditional access/denial authorization decisions).

8. Regarding claims 48 and 71, Cooper teaches wherein said security policy comprises a definition of various objects of said computer network (column 8, lines 44-49, i.e. gross characteristics of the network such as policy domains, communities of hosts, servers, subnets and firewalls).

9. Regarding claims 49 and 72, Cooper teaches wherein said security policy comprises a definition of various services of said computer network (column 8, lines 49-51, i.e. various server services).

10. Regarding claims 50 and 73, Cooper teaches wherein said security policy comprises a definition of various users of said computer network (column 8, lines 44-52, i.e. communities of

hosts).

11. With regards to claims 51 and 74, Cooper teaches generating configuration parameters, thereby enabling the configuration of said portable agents based on said users of said computer network (column 8, lines 44-52, column 13, lines 7-33).

12. Regarding claims 52 and 75, Cooper teaches wherein said security policy comprises a definition of said device (column 8, lines 44-52, column 13, lines 7-33).

13. Regarding claims 53 and 76, Cooper teaches wherein said computer language is a low-level language that is dedicated to operations on said data packets of said computer network, thereby monitoring and limiting the possible actions of said portable agents inside said device (column 4, lines 15-23, column 8, line 60 to column 9, line 47, column 15, lines 7-47).

14. Regarding claims 54 and 77, Cooper teaches defining said security policy in a server remote from said device (Figure 1A [block 106], column 9, lines 52-64).

15. Regarding claim 55, Cooper teaches defining said security policy in said device (Figure 1A [block 110], column 4, lines 24-44, column 8, lines 40-58, column 14, line 25 to column 15, line 4, column 41, lines 53-57, column 43, lines 27-45).

16. Regarding claims 60 and 83, Cooper teaches executing functions from a function library of said software and called by said executable agents (column 9, lines 52-60, i.e. a DLL).

17. With regards to claims 61 and 84, Cooper teaches executing specialized functions from said function library for managing a cache of said data packets (Figure 1A [block 126], column 7, lines 25-36, i.e. capturing and storing packets).

18. With regards to claims 63 and 86, Cooper teaches executing specialized functions from said function library for managing said computer network and transport layers of the communication protocol used (column 4, lines 24-44).

19. Concerning claims 64 and 87, Cooper teaches executing specialized functions comprises the steps of:

storing protocol information from said computer network and said transport layers of said data packets passing through said device to monitor various flows of said data packets (Figure 1A [block 126], column 7, lines 25-36);

storing any modifications of said data packets performed by said executable agents (column 9, lines 16-30, column 40, lines 29-31);

updating said protocol information from said computer network and said transport layers of said data packets passing through said device, based on said protocol information and said stored modifications, in said data packets so as to maintain consistency in the flows of said data packets (column 12, lines 22-39, i.e. editing a security policy).

20. With regards to claims 65 and 88, Cooper teaches executing specialized functions from said function library for searching for regular patterns and expressions (column 3, lines 54-60, column 4, lines 45-49).

21. With regards to claims 66 and 89, Cooper teaches executing specialized functions from said function library for communicating between said executable agents (column 9, lines 52-60, column 16, lines 27-39).

22. With regards to claims 67 and 90, Cooper teaches executing specialized functions from said function library for communicating between said executable agents and objects of said computer network (column 9, lines 52-60, column 16, lines 27-39).

23. With regards to claims 68 and 91, Cooper teaches associating specialized hardware components of said device with functions of said function library to accelerate the execution of said functions (column 9, lines 52-60, column 16, lines 27-39).

24. Regarding claims 69 and 92, Cooper teaches modifying said security policy by executing said executable agents by said processor (column 12, lines 22-39, i.e. editing a security policy).

25. Regarding claim 78, Cooper teaches wherein said device comprises an administrative module for defining said security policy (Figure 1 [block 110], column 4, lines 24-44, column 8,

lines 40-58, column 14, line 25 to column 15, line 4, column 41, lines 53-57, column 43, lines 27-45).

Claim Rejections - 35 USC § 103

26. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claims 56-59 and 79-82 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper in view of U.S. Patent No. 6,941,472 B2 to Moriconi et al., hereinafter Moriconi.

28. Regarding claims 56 and 79, Cooper does not teach authenticating the non-authenticated user of said device to provide an authenticated user of said device.

29. Moriconi teaches authenticating the non-authenticated user of said device to provide an authenticated user of said device (column 1, line 66 to column 2, line 35).

30. It would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate the non-authenticated user of said device to provide an authenticated user of said device, since Moriconi states at column 2, lines 2-5 that authentication ensures that users are part of the organization or a member of the selected group, thereby making it more difficult for unauthorized users to gain access to the system.

31. With regards to claims 57 and 80, Cooper teaches wherein said security policy comprises a definition of said authenticated user of said device (column 8, lines 44-52, i.e. communities of hosts).

32. Concerning claims 58 and 81, Cooper teaches wherein the step of authenticating uses an identification means associated with said device to authenticate said non-authenticated user of said device (column 23, lines 15-67, i.e. using IP and/or MAC addresses).

33. Concerning claims 59 and 82, Moriconi teaches wherein the step of authenticating uses a server application of a client/server application in said device to authenticate said non-authenticated user of said device (column 1, line 66 to column 2, line 35).

Allowable Subject Matter

34. Claims 65 and 82 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

35. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

36. The following patents are cited to further show the state of the art with respect to firewall devices with compilers, such as:

United States Patent Application Publication No. 2003/0120955 A1 to Bartal et al., which is cited to show a firewall that uses a compiler to compile various models for configuring said firewall.

United States Patent No. 7,146,639 B2 to Bartal et al., which is cited to show a firewall that uses a compiler to compile various models for configuring said firewall.

United States Patent No. 6,400,707 B1 to Baum et al., which is cited to show a real-time firewall that compiles configuration files.

United States Patent No. 7,051,365 B1 to Bellovin, which is cited to show a distributed firewall that uses a compiler for compiling a uniform security policy.

United States Patent Application Publication No. 2005/0018682 A1 to Ferguson et al., which is cited to show a method for processing packets using a compiler that compiles data used to process said packets.

United States Patent No. 6,798,777 B1 to Ferguson et al., which is cited to show a method for processing packets using a compiler that compiles data used to process said packets.

United States Patent No. 7,257,833 B1 to Parekh et al., which is cited to show a policy compiler for firewalls that produces infrastructure module data file and policy module data files.

United States Patent Application Publication No. 2005/0091515 A1 to Roddy et al., which is cited to show compiling policies set by the administrator that are used for firewall mediation.

United States Patent Application Publication No. 2006/0253901 A1 to Roddy et al., which is cited to show compiling policies set by the administrator that are used for firewall mediation.

United States Patent No. 7,043,753 B2 to Roddy et al., which is cited to show compiling policies set by the administrator that are used for firewall mediation.

United States Patent No. 6,845,452 B1 to Roddy et al., which is cited to show compiling policies set by the administrator that are used for firewall mediation.

United States Patent No. 6,779,120 B1 to Valente, which is cited to show a patent that was incorporated by reference in the Cooper reference above.

37. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

38. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

39. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

clf